Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases

Viktor Levandovskyy, Kristina Schindelar
Lehrstuhl D für Mathematik, RWTH Aachen,
Templergraben 64, 52062 Aachen, Germany
[Viktor.Levandovskyy,Kristina.Schindelar]@math.rwth-aachen.de

March 22, 2010

Abstract

In this paper we present two algorithms for the computation of a diagonal form of a matrix over non-commutative Euclidean domain over a field with the help of Gröbner bases. This can be viewed as the preprocessing for the computation of Jacobson normal form and also used for the computation of Smith normal form in the commutative case. We propose a general framework for handling, among other, operator algebras with rational coefficients. We employ special "polynomial" strategy in Ore localizations of non-commutative G-algebras and show its merits. In particular, for a given matrix M we provide an algorithm to compute U, V and D with fraction-free entries such that $UMV = D$ holds. The polynomial approach allows one to obtain more precise information, than the rational one e. g. about singularities of the system.

Our implementation of polynomial strategy shows very impressive performance, compared with methods, which directly use fractions. In particular, we experience quite moderate swell of coefficients and obtain uncomplicated transformation matrices. This shows that this method is well suitable for solving nontrivial practical problems. We present an implementation of algorithms in Singular:Plural and compare it with other available systems. We leave questions on the algorithmic complexity of this algorithm open, but we stress the practical applicability of the proposed method to a bigger class of non-commutative algebras.

Contents

1 Introduction

The existence and computation of normal forms of matrices over a ring is a fundamental mathematical question. The proof for the existence of a normal form is mainly constructive and can be turned into an algorithm. However, such a direct algorithm is not very efficient in general. Computer algebra focuses its attention on this kind of problems, since they are of elementary interest but of high complexity.

In that sense nearly any computer algebra system is able to compute the Smith normal form for a matrix over a commutative principal ideal domain ($\mathbb{Z}$ or $K[x]$ for a field K). There are many textbooks giving a theoretical background, like for instance [10, 29].

We present a method, which is based on Gröbner bases. In [19], there is a Gröbner basis-based algorithm for the computation of Smith normal form of a matrix with entries in $K[x]$. Despite the fact that this approach seems to be folklore, we were not able to find other references.

In this paper we consider non-commutative skew polynomial rings. Such rings, among other, offer the possibility to describe time varying systems in Systems and Control theory [32], [17], [18]. Many known operator algebras can be realized as skew polynomial rings or solvable polynomial rings [22], some of them can be realized even as much easier Ore algebras [9, 8]. However, general solvable polynomial rings are hard to tackle constructively (say, in a computer algebra system), while the class of Ore algebras of [9, 8] is indeed restrictive. Based on the PBW algebras [5] also known as G-algebras [23, 15], in Section 2 we propose a new class of univariate skew polynomial rings, which are obtained as Ore localizations of G-algebras. This framework is powerful and convenient at the same time. Moreover, it is more general than the class of Ore algebras (with defining endomorphism σ being an automorphism) and allows algorithmic treatment of modules. In Proposition 2.2 and Theorem 2.6 several nice properties of such algebras (among other, these algebras are Noetherian domains with PBW basis) are established. We stress, that the computations in these algebras, especially Gröbner bases for modules, are algorithmic and, moreover, they can be done without using explicit fractions. It is important, that such algebras and computations in them can be realized in any computer algebra system, which can handle G-algebras or polynomial Ore algebras.

In [11], applications to systems of partial differential equations are shown and

several concrete examples are introduced. We generalize the idea, originating from [19], to use Gröbner bases in computation of normal forms for matrices. The crucial improvement is introduced in Section 3.3, where we show how to handle the problem in a completely fraction-free polynomial framework.

We point out advantages of the polynomial strategy and illustrate some of them with interesting examples in the Section 4, where we compare our implementation with other available packages. In particular, we do comparisons with the implementation of algorithms, which use fractions directly. Notably, in many examples our approach delivers much more compact results with small coefficients.

The non-commutative analogue to the Smith form over a principal ideal domain is the Jacobson form [20] ,[10]. However, since the normal form problem is hard in general, we propose the notion of a weak Jacobson form, that is a diagonal matrix, where the units on the diagonal will not be necessarily generated. Otherwise the advantage of the polynomial strategy is disturbed. Instead, we propose the splitting of the whole process of obtaining a (strong) normal form into the computation of a diagonal form and the computation of stronger diagonal form from a given diagonal one. The latter, as we show in 4.4, 4.5 and 4.6 depends heavily on the domain one computes in, while the first algorithm is very general.

Our implementation (of weak Jacobson and Smith forms) is realized as the library `jacobson.lib` [30] for the computer algebra system SINGULAR:PLURAL [16, 15], which is freely available. The library has been already incorporated into the official distribution of SINGULAR version 3-1-0.

2 Algebras, Localizations and their Properties

The framework of this paper is based on skew polynomial rings that are principal ideal domains. An important subclass of skew polynomial rings constitute so-called polynomial Ore rings. They are non-commutative rings possessing an endomorphism σ and a σ-derivation to define the commutation rule of two elements, that is giving the extension from commutative polynomial ring to non-commutative. This kind of rings is used in analyzing the structure of analytic equations, like linear ordinary or partial differential equations or partial shift or difference equations with rational or polynomial coefficients, see Example 2.3. The name is inspired by Øystein Ore, who introduced and studied this kind of rings. These rings were also studied, for instance in [9] and [27].

Let K be a field and A be a K-algebra. Further let $\sigma : A \to A$ be a ring endomorphism. Then the map $\delta : A \to A$ is called σ-**derivation**, if δ is K-linear and satisfies the skew Leibniz rule

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b \ \text{ for all } \ a, b \in A.$$

For a σ-derivation δ the ring $A[\partial; \sigma, \delta]$ consisting of all polynomials in ∂ with coefficients in A with the usual addition and a product defined by the commu-

tation rule

$$\partial a = \sigma(a)\partial + \delta(a) \ \text{ for all } \ a \in A$$

is called **skew polynomial ring** or an **Ore extension** of A with ∂ subject to σ, δ.

It is easy to see, that any non-zero element $a \in A[\partial; \sigma, \delta]$ can be written as $a = a_n \partial^n + \cdots + a_1 \partial + a_0$, where $n \in N_0$ and $a_i \in A$. We call n the **degree** of a, sometimes it is also called the **order** of a.

In describing K-algebras via finite sets of generators G and relations R, we write $A = K\langle G \mid R \rangle$. It means that A is a factor algebra of the free associative algebra, generated by G modulo the two-sided ideal, generated by R. Hence yet another notation is $A = K\langle G \rangle / \langle R \rangle$.

Example 2.1.

- Defining $\sigma := \mathrm{id}_A$ and $\delta := 0$ we see, that $(K[x_1, \ldots, x_n])[\partial; \sigma, \delta] = K[x_1, \ldots, x_n, \partial]$ and $K(x_1, \ldots, x_n)[\partial; \sigma, \delta] = K(x_1, \ldots, x_n)[\partial]$.

- Let $A = K[x]$ for a field K of characteristic 0, $\sigma := \mathrm{id}_{K[x]}$ and $\delta := \frac{\partial}{\partial x}$.

$$W_1(K) := K[x][\partial; \mathrm{id}_{K[x]}, \frac{\partial}{\partial x}] = K\langle x, \partial \mid \partial x = x\partial + 1 \rangle$$

  is called the first **polynomial Weyl algebra**.

Proposition 2.2. [5] Let A be a division ring, $\sigma : A \to A$ be an endomorphism and $R = A[\partial; \sigma, \delta]$ be an Ore extension with a σ-derivation δ.
If σ is injective (respectively bijective), then

- (PID) R is a left (resp. right) principal ideal domain.

- (Bezout's Theorem) for any non-zero $a, b \in R$ there exists the right (resp. left) greatest common divisor g_r (resp. g_ℓ) of a, b and there exist $s, t \in R$, such that $g_r = sa + tb$ (resp. s', t', such that $g_\ell = as' + bt'$).

- (ED) R is a left (resp. right) Euclidean domain.

Hence, when σ is bijective, there are left and right Euclidean division algorithms.

In the next example we enlist some interesting skew polynomial rings (which are Ore algebras indeed, see [9]). These rings are of great interest in applications, all of them can be addresses with our implementation, see Section 4.

Example 2.3. Let $A = K(x)$, where K is a field of characteristic 0.

- Let $\sigma := \mathrm{id}_{K(x)}$ and $\delta := \frac{\partial}{\partial x}$. Then

$$B_1(K) := A[\partial; \mathrm{id}_{K(x)}, \frac{\partial}{\partial x}] = K(x)\langle \partial \mid \partial x = x\partial + 1 \rangle$$

  is called the first **rational Weyl algebra**.

4

- The first **rational difference algebra** is defined by

$$\mathcal{S}_1 := A\,[\Delta; \sigma, \delta] = K(x)\langle \Delta \mid \Delta x = x\Delta + \Delta + 1\rangle,$$

  where $\sigma(p(x)) = p(x+1)$ and $\delta(p) = \sigma(p) - p$ for all $p \in K(x)$.

Let $q \neq 0$ be a unit (a parameter) in the ground field.

- Let $\sigma(p(x)) = p(qx)$ and $\delta := (\frac{\partial}{\partial x})_q$, $\delta(f(x)) = \frac{f(qx) - f(x)}{(q-1)x}$. Then

$$W_1^q(K) := A[\partial; \sigma, (\tfrac{\partial}{\partial x})_q] = K(x)\langle \partial \mid \partial x = q \cdot x\partial + 1\rangle$$

  is called the first **rational q-Weyl algebra**.

- The first **rational q-difference algebra** is defined by

$$\mathcal{Q} := A[\partial; \sigma, \delta] = K(x)\langle \partial \mid q \cdot x\partial + (q-1)x\rangle,$$

  where $\sigma(p) = p(qx)$ and $\delta(p) = p(qx) - p(x)$.

Indeed, we can work within the more general algebraic framework as follows.

Let S be a multiplicatively closed set (see [27]) in a Noetherian integral domain A, such that $0 \notin S$. S is called an **Ore set** in A, if for all $s_1 \in S, a_1 \in A$ there exist $s_2 \in S, a_2 \in A$, such that $a_1 s_2 = s_1 a_2$. Then one can see, that formally (that is, allowing fractional expressions) $s_1^{-1} a_1 = a_2 s_2^{-1}$ holds.

Then one defines a **ring of fractions** or an **Ore localization** of A with respect to S to be a ring A_S (often denoted as $S^{-1}A$) together with an injective homomorphism $\phi : A \to A_S$, such that

(i) for all $s \in S$, $\phi(s)$ is a unit in A_S,

(ii) for all $f \in A_S$, $f = \phi(s)^{-1}\phi(a)$ for some $a \in A, s \in S$.

The Ore property of S in A guarantees, that any left-sided fraction can be written (non-uniquely!) as a right-sided fraction. Moreover, given $a_1, \ldots, a_m \in A$ and $s_1, \ldots, s_m \in S$, there exist $a_1', \ldots, a_m' \in A$ and $s' \in S$, such that $a_i s' = s_i a_i'$ holds for each i. Thus there exist common right and common left multiples.

Remark 2.4. Why such localizations are important? Among many motivating connections let us state the following. Given an A-module homomorphism $\varphi : M \to N$, where M, N are finitely generated. Then, if $S^{-1}A$ exists, one has an induced homomorphism of $S^{-1}A$-modules $S^{-1}\varphi : S^{-1}M \to S^{-1}N$. However, if one finds an appropriate multiplicatively closed Ore set $\tilde{S}$ in A and proves that $\tilde{S}^{-1}\varphi : \tilde{S}^{-1}M \to \tilde{S}^{-1}N$ is not an isomorphism, it implies that $M \not\cong N$ as A-modules. This gives an important tool to check the isomorphy of modules. In contrast with common localizations of commutative ring at complements of prime ideals, we do not know a priori for which S we are looking for and how many different S should we examine.

Note, that the question, whether two modules are isomorphic, is one of the fundamental questions in algebra. It is known to be not algorithmic in general, hence any partial algorithmic answer to this question is of big importance.

Definition 2.5. Let A be a quotient of the free associative algebra $K\langle x_1, \ldots, x_n \rangle$ by the two-sided ideal I, generated by the finite set $\{x_j x_i - c_{ij} x_i x_j - d_{ij}\}$ for all $1 \le i < j \le n$, where $c_{ij} \in K^*$ and d_{ij} are polynomials in $x_1, \ldots, x_n$. Without loss of generality [23] we can assume that d_{ij} are given in terms of standard monomials $x_1^{a_1} \ldots x_n^{a_n}$. A is called a G–*algebra* [24, 23], if
- for all $1 \le i < j < k \le n$ the expression $c_{ik} c_{jk} \cdot d_{ij} x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik} x_j + d_{jk} x_i - c_{ij} c_{ik} \cdot x_i d_{jk}$ reduces to zero modulo I and
- there exists a monomial ordering $\prec$ on $K[x_1, \ldots, x_n]$, such that for each $i < j$, such that $d_{ij} \ne 0$, $\operatorname{lm}(d_{ij}) \prec x_i x_j$. Here, lm stands for the classical notion of leading monomial of a polynomial from $K[x_1, \ldots, x_n]$.

We call an ordering on a G-algebra **admissible**, if it satisfies second condition of the definition. A G-algebra A is Noetherian integral domain [24], hence there exists its total two-sided ring of fractions $\operatorname{Quot}(A) = A_{A \setminus \{0\}}$, which is a division ring (skew field). Assume that A is generated by $x_1, \ldots, x_{n+1}$ and suppose that the set $\Lambda_n(A) = \{\lambda = \{i_1, \ldots, i_n\} \mid i_1 < \ldots < i_n, K\langle x_{i_1}, \ldots, x_{i_n} \mid I_\lambda\rangle$ is a G-algebra$\}$ is not empty, where $I_\lambda = \{x_j x_i - c_{ij} x_i x_j - d_{ij} \mid i, j \in \lambda, i < j\}$.

For any $\lambda = \{i_1, \ldots, i_n\} \in \Lambda_n$, let us define B_λ to be a G-algebra, generated by $\{x_{i_1}, \ldots, x_{i_n}\}$.

Theorem 2.6. Let A be a G-algebra in variables $x_1, \ldots, x_n, \partial$ and assume that $\lambda = \{x_1, \ldots, x_n\} \in \Lambda_n$. Moreover, let $B := B_\lambda$ and $B^* = B \setminus \{0\}$. Suppose, there exists an admissible monomial ordering $\prec$ on A, satisfying $x_k \prec \partial$ for all $1 \le k \le n$. Then the following holds

- B^* is multiplicatively closed Ore set in A.

- $(B^*)^{-1} A$ (Ore localization of A with respect to B^*) can be presented as an Ore extension of $\operatorname{Quot}(B)$ by the variable ∂.

Proof. Since B is a G-algebra itself, it is an integral domain, hence B^* is multiplicatively closed and does not contain zero. Since A and B are G-algebras and $\prec$ is an admissible ordering, for a relation $\partial x_j = c_j x_j \partial + d_j$ with $c_j \in K^*$ and a polynomial $d_j \in A$ holds $d_j = 0$ or $\operatorname{lm}(d_j) \prec x_j \partial$. Since $x_j \prec \partial$, then $x_j \partial \prec \partial^2$, hence d_j is at most linear in ∂. Writing $d_j = a_j \cdot \partial + b_j$ for $a_j, b_j \in B$, we define $c_j' = c_j x_j + a_j$ and thus we obtain a relation $\partial x_j = c_j' \partial + b_j$, where $x_j, c_j', b_j \in B$.

Then, by defining $\sigma(x_j) = c_j x_j + a_j$ and $\delta(x_j) = b_j$ for all $1 \le j \le n$, we see, that σ is an automorphism of $\operatorname{Quot}(B)$. Thus an Ore extension $\operatorname{Quot}(B)[\partial; \sigma, \delta]$ is indeed another presentation of $(B^*)^{-1} A$ as soon as B^* is an Ore set in A.

Since $\operatorname{lm}(d_j) = \operatorname{lm}(a_j \partial + b_j) \prec x_j \partial$, both $\operatorname{lm}(a_j) \prec x_j$ and $\operatorname{lm}(b_j) \prec x_j \partial$ hold. The latter implies, that there exist positive weights ω and $w_1, \ldots, w_n$ for variables $\{\partial, x_1, \ldots, x_n\}$, such that for $\operatorname{lm}(a_j) = x^\alpha$ and $\operatorname{lm}(b_j) = x^\beta$ one has $\sum_i w_i \alpha_i \le w_j$ and $\sum_i w_i \beta_i \le w_j + \omega$. In particular, this can be achieved by setting ω big enough. Then we follow the recipe from [5] and construct a block ordering from this setting. Consider an ordering $\prec_\partial$ on A, which is a block ordering for blocks of variables $\{\partial\}, \{x_1, \ldots, x_n\}$. It means that $\partial \gg x_j$ for all j, that is the variable ∂ is bigger than any power of x_j. The second block is an

6

ordering $\prec_B$ on B, for which $\mathrm{lm}(a_j) \prec_B x_j$ holds. For instance, one can take $\prec_B$ to be the restriction of $\prec$ to B. Then $\mathrm{lm}(d_j) = \max_{\prec_\partial}(a_j \partial, b_j) \prec_\partial x_j \partial$ holds, hence $\prec_\partial$ is admissible ordering on A. From the Proposition 28 of [13] (which holds for much more general situation), the existence of such a block ordering as $\prec_\partial$ implies, that the set B^* is an Ore set in A. $\qquad\square$

Remark 2.7. Note, that by construction $A_{B^*} := (B^*)^{-1} A$ is a Euclidean (principal ideal) domain by the Proposition 2.2. In particular, all but one variables are invertible (we call them also *rational* variables). We call non-invertible variables *polynomial*. In a more general setting, we like to present localizations of the type A_{B^*}, where B is a sub-G-algebra of A, as a ring of solvable type [22] or, equivalently, as a PBW ring [5]. In the case of several polynomial variables, the analogue to the Theorem 2.6 seem to be much more involved.

Example 2.8. To illustrate the Theorem 2.6, consider the difference algebra $\mathcal{S}_1 := K\langle x, \Delta \mid \Delta x = x\Delta + \Delta + 1\rangle$. Since $\Delta \prec x\Delta$ is a consequence of $1 \prec x$ (we assume we are dealing with well-orderings only), $\mathcal{S}_1$ can be localized at both $K[x]^*$ and $K[\Delta]^*$. However, the algebra, associated with the operator of partial integration $\mathcal{I}_1 := K\langle x, I \mid Ix = xI - I^2\rangle$ can be localized only at $K[I]^*$ but not at $K[x]^*$, since $I^2 \prec xI$ is a consequence of $I \prec x$ and any ordering, satisfying $x \prec I$ is not admissible for $\mathcal{I}_1$.

For many problems in module theory and in applications we would like to analyze complicated problems via localizing at big subalgebras. In the situation as above, we obtain non-commutative Euclidean domain as the result, hence we are interested in computing Jacobson form in this setting. One of the complications, which arise in constructive handling of objects over such algebras, is quite hard arithmetics in the skew field. Several fundamental questions like the transformation of a left fraction into the right one (which is possible, since the Ore condition is satisfied), simplification of a one-sided fraction etc. require quite nontrivial and complex algorithms (like computation of syzygy modules and so on) to be used, see for instance [1]. Even in the commutative case the computations (even with one variable) over a transcendental extension by several generators are still nontrivial and resource-consuming for most computer algebra systems. Hence saying "ring R is a (non-commutative) Euclidean domain" does not automatically mean "computations in R are easy".

Remark 2.9. Let us come back to the justification of terminology. Usually, speaking on "operator algebra with polynomial coefficients", one means that one works with the set of operators $\partial_1, \ldots, \partial_m$ over a commutative polynomial ring, say, $K[x_1, \ldots, x_n]$.

By saying "operator algebra with rational coefficients" one addresses an Ore extension of $K(x_1, \ldots, x_n)$ by the operators ∂_i.

It is important to mention, that $K(x_1, \ldots, x_n)$ is a localization of $K[x_1, \ldots, x_n]$ with respect to multiplicatively closed set $K[x_1, \ldots, x_n] \setminus \{0\}$. Thus it is enough to define an algebra with polynomial coefficients and then speak on different localizations of it. Therefore the notion of Ore localization reveals the origin of

7

various "rational" coefficients and allows to treat different localizations (among them e.g. passage to the torus $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] \subset K(x_1, \ldots, x_n)$) uniformly.

3   Gröbner Bases in the Computation of a Diagonal Form

3.1   Yoga with Gröbner Bases

Let us give a short introduction to non-commutative Gröbner basis theory, which has been studied by e. g. [7, 22, 23]. Suppose, that there is a G-algebra R_* over a field K, which is generated by $x_1, \ldots, x_n, \partial$, such that $R_* = A_*[\partial; \sigma, \delta]$ is an Ore extension of a G-algebra A_*, generated by $\{x_i\}$. By using the lower index $*$, we point out that we deal with structures, objects in which always have a polynomial presentation. A nice property of a G-algebra is that as a K-vector space it is generated by **monomials** of R_*:

$$\mathrm{Mon}(R_*) = \{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \partial^k \mid \alpha \in \mathbb{N}^n, k \in \mathbb{N}\} = \{x^\alpha \partial^k \mid x^\alpha \in \mathrm{Mon}(A_*), k \in \mathbb{N}\}.$$

Based on a module ordering we define leading coefficient (lc), leading monomial (lm), leading term (lt) and leading position (lpos) notions as usual. Let $e_i := (0, \ldots, 1, \ldots, 0)$ be the i-th unit vector.

In this paper we will compute Gröbner basis of modules over R_* with respect to an monomial module ordering POT (position-over-term), defined as follows. For $r, s \in \mathrm{Mon}(R_*)$,

$$re_i < se_j \quad \Leftrightarrow \quad i < j \text{ or if } i = j \text{ then } r < s, \tag{1}$$

and $r < s$ with respect to an admissible well-ordering on R_*, eliminating ∂, that is satisfying $\partial \gg x_n > \cdots > x_1$ on R_*.

In R, a Gröbner basis is computed with respect to the induced POT ordering, which takes only degree of ∂ into account since $\mathrm{Mon}(R) = \{\partial^k \mid k \in \mathbb{N}\}$.

We call $a \in R_*$ a **strict left (resp. right) divisor** of $b \in R_*$ if and only if $\exists\, f \in R_*$ such that $af = b$ (resp. $fa = b$). Extending this notation to R_*^p requires that both elements $a, b \in R_*^p$ have the same leading position. Moreover, a is said to be a **proper** strict divisor of b, if either $b = af$ or $b = fa$ holds, where f is not an unit in R_*. For two monomials $m_1, m_2 \in R_*$ we write $m_1 \leq m_2$ for the comparison with the fixed monomial ordering. We say that m_1 **divides** m_2, if each exponent of m_1 is not greater than the corresponding exponent of m_2.

Definition 3.1. Let M be a left submodule of R_*^p and $<$ be a monomial module ordering on R_*^p. A finite subset $G \subset M$ is called a **Gröbner Basis** of M with respect to $<$, if for every $f \in M \setminus \{0\}$ there exists a $g \in G$, so that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$.

A Gröbner basis G is called **reduced** if and only if for any pair of polynomials $h \neq f \in G$, the leading monomial $\mathrm{lm}(h)$ does not divide any monomial of f. It can be shown, that a normalized (that is with leading coefficients 1) reduced

Gröbner basis is unique for a fixed ordering. We recall the common property of a Gröbner basis to be, in particular, a generating set.

Remark 3.2. Let $M \subseteq R_*^p$ with a Gröbner basis G and $f \in M$. Define the submodule S of M to be generated by all $s \in G$ such that $\mathrm{lm}(s) \leq \mathrm{lm}(f)$. Then $f \in S$.

3.2 Working with Left and Right Modules

Opposite algebra. In order to work with left and right modules over an associative K-algebra A, one has to use both A and its opposite algebra A^{op} in general. Recall, that A^{op} is the same vector space as A, endowed with the opposite multiplication: $\forall\ a, b \in A^{op}$, $a \star_{A^{op}} b = b \cdot a$. A natural opposing map makes from a right (resp. left) A-module a left (resp. right) A^{op}-module. There is an algorithmic procedure to set up an opposite algebra to a given G-algebra, see [23].

Involutive anti-automorphism. Alternatively, for "swapping sides" one can employ an anti-automorphism θ of A , that is a K-linear map, which obeys $\theta(ab) = \theta(b)\theta(a)$ for all $a, b \in A$, which is involutive, that is $\theta^2 = \mathrm{id}_A$. Often such an anti-automorphism is called **involution**. In classical operator algebras, particularly simple involutions are known [8]. Moreover, it is possible to determine linearly presented involution of a G-algebra via an algorithm (Levandovskyy et al., unpublished, see SINGULAR library `involut.lib` [2] for an implementation). A constructive advantage of using involution versus using opposite algebra lies in the fact, that one does not need to create opposite algebra and make to an object its opposite. Instead, we apply an involution to an object and remain in the same ring. One application of involution means that the object we deal with change its side from left to right or vice versa.

An involution can be defined on matrices as follows. Let $\theta : A \to A$ be an involution as above. We define the map

$$\widetilde{\theta} : A^{p \times q} \to A^{q \times p}, \quad M \mapsto (\theta(M))^T,$$

where M^T is the transposed matrix of M and $\theta(M) = [\theta(M_{ij})]$ for $1 \leq i \leq p$ and $1 \leq j \leq q$.
One can easily show that $(\theta(B \cdot C))^T = (\theta(C))^T \cdot (\theta(B))^T$ for $B \in A^{p \times q}$, $C \in A^{q \times k}$. Applied twice, we get $B \cdot C$ back.

Diagonalization. Let R be a K-algebra and a non-commutative Euclidean PID. Recall, that a matrix $U \in R^{p \times p}$ is called **unimodular** if and only if there exists $U^{-1} \in R^{p \times p}$ such that $UU^{-1} = U^{-1}U = \mathrm{id}_{p \times p}$. Let $M \in R^{p \times q}$ and assume, without loss of generality, that $p > q$. Then one can show, that there

exist unimodular matrices $U \in R^{p \times p}$ and $V \in R^{q \times q}$ such that

$$
UMV = \begin{bmatrix} m_1 & & & 0 \\ & \ddots & & \\ 0 & & m_q & \\ & & 0_{p-q} & \end{bmatrix}.
$$

There are several ways to prove this statement, all based on the Euclidean (and thus PID) property of the underlying ring. From now on, we assume that R is a localization of a G-algebra as in Remark 2.7. We present algorithms to obtain diagonal form together with unimodular transformation matrices via Gröbner bases. The main idea about the computation is the sequential alternation between the computation of a reduced Gröbner basis of the submodule, generated by, say, the rows of a matrix and acting by the involution $\widetilde{\theta}$ on a submodule. In the PhD thesis [19] this idea was applied to $K[x]$ (of course, without using an involution θ, which is superfluous in that case) in order to compute a Smith normal form.

In the following, by $_RM$ we denote the left R-module generated by the rows of a matrix M. Further on, by $\mathcal{G}(_RM)$ we denote the reduced left Gröbner basis of the submodule, generated by $_RM$ with respect to the module ordering (1).

For the i-th row of a matrix M we write M_i and M_{ij} stands, as usual, for the entry in the i-th row and j-th column. With respect to the context we identify $\mathcal{G}(_RM) = \{g_1, \ldots, g_m\}$ with the matrix $[g_1^t, \ldots, g_m^t]^t$. Define the **degree** of an element $0 \neq m \in R^{1 \times q}$ to be the degree of the corresponding leading monomial, that is, $\deg(m) := \deg(\operatorname{lm}(m))$. Since R is a PID, this degree measures the highest exponent in the variable ∂. Following the standard convention, $\deg(0) = -\infty$. Note that the elements of $\mathcal{G}(_RM)$ have pairwise distinct leading monomials, since they form a reduced Gröbner basis. In a reduced Gröbner basis $\operatorname{lm}(\mathcal{G}(_RM)_i) \mid \operatorname{lm}(\mathcal{G}(_RM)_j)$ if and only if $\mathcal{G}(_RM)_i = \mathcal{G}(_RM)_j$.

Lemma 3.3. Order a reduced Gröbner basis in such a way, that $\operatorname{lm}(\mathcal{G}(_RM)_1) < \cdots < \operatorname{lm}(\mathcal{G}(_RM)_m)$. Then

$$
\begin{bmatrix} \mathcal{G}(_RM)_1 \\ \vdots \\ \mathcal{G}(_RM)_m \end{bmatrix}
$$

is a lower triangular matrix.

Proof. Suppose the claim does not hold. Then there exists $\mathcal{G}(_RM)_i$ and $\mathcal{G}(_RM)_j$ with $\operatorname{lpos}(\mathcal{G}(_RM)_i) = \operatorname{lpos}(\mathcal{G}(_RM)_j)$ for $i < j$. Thus $\operatorname{lm}(\mathcal{G}(_RM)_i) = \partial^{\alpha_i} e_k$ and $\operatorname{lm}(\mathcal{G}(_RM)_j) = \partial^{\alpha_j} e_k$ such that $\alpha_i < \alpha_j$. But then evidently $\operatorname{lm}(\mathcal{G}(_RM)_i)$ divides $\operatorname{lm}(\mathcal{G}(_RM)_j)$, which is a contradiction to $\mathcal{G}(_RM)$ being reduced. $\square$

Due to the previous lemma, we may assume without loss of generality, that the matrix $\mathcal{G}(_RM)$ is lower triangular. Since R is an integral domain, we define

the rank of a matrix M to be the rank of M over the field of fractions of R. Now, let us assume that $p = q$ and M is of full rank, that is row and column ranks of M are equal to p. The non-square case will be discussed in Remark 3.7.

Lemma 3.4. Let $\mathcal{I}$ denote the left ideal generated by the elements in the last column of $\widetilde{\theta}(\mathcal{G}(_RM))$, that is, by $\theta(\mathcal{G}(_RM)_{p1}), \dots, \theta(\mathcal{G}(_RM)_{pp})$. Then

$$\mathcal{I} = {_R}\langle \mathcal{G}(_R\widetilde{\theta}(\mathcal{G}(_RM)))_{pp} \rangle.$$

Proof. Note, that due to Lemma 3.3

$$\underbrace{\begin{bmatrix} * & & \\ \vdots & \ddots & \\ \mathcal{G}(_RM)_{p1} & \cdots & \mathcal{G}(_RM)_{pp} \end{bmatrix}}_{\mathcal{G}(_RM)} \overset{\widetilde{\theta}}{\rightsquigarrow} \begin{bmatrix} & & \theta(\mathcal{G}(_RM)_{p1}) \\ & \cdot^{\cdot^{\cdot}} & \vdots \\ * & \cdots & \theta(\mathcal{G}(_RM)_{pp}) \end{bmatrix} \overset{\mathcal{G}}{\rightsquigarrow} \begin{bmatrix} * & & \\ \vdots & \ddots & \\ * & \cdots & \mathcal{G}(_R\widetilde{\theta}(\mathcal{G}(_RM)))_{pp} \end{bmatrix}.$$

According to the definition of $\mathcal{G}$ the left ideal generated by $\mathcal{G}(_R\widetilde{\theta}(\mathcal{G}(_RM)))_{pp}$ coincides with $_R\langle \theta(\mathcal{G}(_RM)_{p1}), \dots, \theta(\mathcal{G}(_RM)_{pp}) \rangle$. $\square$

Now we can formulate the algorithm that yields the desired diagonal form.

Algorithm 3.5 (`Diagonalization with Gröbner Bases`).
Input: $M \in R^{g \times g}$ of full rank, $\widetilde{\theta}$ involution as above.
Output: Matrices $U, V, D \in R^{g \times g}$, such that

$$U, V \text{ are unimodular and } U \cdot M \cdot V = \mathrm{Diag}(r_1, \dots, r_g) = D.$$

$M^{(0)} \leftarrow M,\ U \leftarrow \mathrm{id}_{g \times g},\ V \leftarrow \mathrm{id}_{g \times g}$
$i \leftarrow 0$
while $(M^{(i)}$ is not a diagonal matrix **or** $i \equiv_2 1)$ **do**
   $i \leftarrow i + 1$
   Compute $U^{(i)}$ such that $U^{(i)} \cdot M^{(i-1)} = \mathcal{G}(_RM^{(i-1)})$
   $M^{(i)} \leftarrow \widetilde{\theta}(\mathcal{G}(_RM^{(i-1)}))$
   if $(i \equiv_2 0)$ **then**
     $V \leftarrow V \cdot \widetilde{\theta}(U^{(i)})$
   else
     $U \leftarrow U^{(i)} \cdot U$
   end if
end while
return $(U, V, M^{(i)})$

Theorem 3.6. The Algorithm 3.5 terminates and it is correct.
That is, for $M \in R^{g \times g}$, let $M^{(i)}$ denote the matrix we get after the i-th execution of the **while** loop. Then there exists an element $k \in \mathbb{N}$ such that $M^{(k)}$ is a diagonal matrix. If k is odd, then the **while** loop is repeated just one more time (define $l := k + (k \mod 2)$ in this case). The matrices U, V obtained in the last loop are unimodular and satisfy $UMV = \mathrm{Diag}(m_1, \dots, m_g)$.

11

Proof. We prove the claim by induction on g, the size of the square matrix M. For $g = 1$ there is nothing to show. Using Lemma 3.4, the equality $_R\langle\theta((M^{(i+1)})_{gg})\rangle = {}_R\langle(M^{(i)})_{1g}, \ldots, (M^{(i)})_{gg}\rangle$ holds. Hence we get

$$_R\langle(M^{(i)})_{gg}\rangle \subseteq {}_R\langle\theta((M^{(i+1)})_{gg})\rangle \quad \text{for all } i.$$

Note that θ preserves the degree. Then the previous inclusion implies by degree arguments that $_R\langle(M^{(r)})_{gg}\rangle = {}_R\langle(M^{(r+1)})_{gg}\rangle$ for some r. Using Lemma 3.4 and $(M^{(r)})_{gg} \neq 0$ (since M is of full rank), we obtain that $(M^{(r)})_{gg}$ is a strict left divisor of $(M^{(r)})_{ig}$ for each $1 \leq i \leq g - 1$. Then the definition of $\mathcal{G}$ yields that

$$M^{(r+1)} = \begin{pmatrix} & & & 0 \\ & M' & & \vdots \\ & & & 0 \\ 0 & \ldots & 0 & (M^{(r+1)})_{gg} \end{pmatrix}.$$

, or, in a different notation, $M^{(r+1)} = M' \oplus (M^{(r+1)})_{gg}$, that is $M^{(r+1)}$ is a block matrix.

The $(g-1) \times (g-1)$ matrix M' can be transformed to a diagonal matrix via unimodular operations by induction. It remains to consider the transformation matrices U and V. For each $i \in \mathbb{N}$, after executing the **while** loop i times, we obtain

$$\begin{cases} M^{(i)} = U^{(i-1)} \cdot U^{(i-3)} \cdots U^{(1)} \cdot M \cdot \widetilde{\theta}(U^{(2)}) \cdot \widetilde{\theta}(U^{(4)}) \cdots \widetilde{\theta}(U^{(i)}), & \text{if } i \text{ is even} \\ M^{(i)} = U^{(i-1)} \cdot U^{(i-3)} \cdots U^{(1)} \cdot \widetilde{\theta}(M) \cdot \widetilde{\theta}(U^{(2)}) \cdot \widetilde{\theta}(U^{(4)}) \cdots \widetilde{\theta}(U^{(i)}), & \text{if } i \text{ is odd}, \end{cases}$$

which completes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Remark 3.7. In order to extend Theorem 3.6 and Algorithm 3.5 to non-square and non-full rank matrices, we need to add suitable syzygies to U respectively V and zero rows respectively columns to the diagonal matrix, in order to maintain the initial size of M. For a computational solution it is sufficient to extend Algorithm 3.5 in the following way. Let $M^i \in R^{s \times t}$ where either $s = p, t = q$ or $s = q, t = p$ in the i-th while loop. Instead of computing U^i, satisfying $U^i \cdot M^{i-1} = \mathcal{G}(_R M^{i-1})$, we compute $\mathcal{G}(_R \tilde{M})$ for the extended matrix $\tilde{M} := [\text{id}_{s \times s} M^{i-1}]$. Such $\tilde{M}$ is obviously a full row rank matrix. Defining $U^i := [\mathcal{G}(_R\tilde{M})_1^T, \ldots, \mathcal{G}(_R\tilde{M})_s^T]^T$ and $M^i := [\mathcal{G}(_R\tilde{M})_{s+1}^T, \ldots, \mathcal{G}(_R\tilde{M})_t^T]^T$, it is easy to see that $U^i M^{i-1} = M^i$. The matrix M^i consists of the rows of $\mathcal{G}(_R M^{i-1})$ and additional zero rows, such that $M^i \in R^{s \times t}$.

3.3 Polynomial Strategy

We are given a matrix M over a non-commutative Euclidean domain R. In this section, we show our main approach of this chapter. We introduce a method that allows to execute the Algorithm 3.5 in a completely polynomial (that is, fraction-free) framework. The idea comes from the commutative case and was appeared e. g. in [14].

Let A_* be a G-algebra and $A = \text{Quot}(A_*)$. Moreover, let $R = A[\partial; \sigma, \delta]$, such that $R_* = A_*[\partial; \sigma, \delta]$ is a G-algebra. Evidently $R_* \subseteq R$, since $A_* \subseteq A$. Without loss of generality, we suppose that M does not contain a zero row.

We define the **degree** of an element in R_* (or $R_*^{1 \times g}$) to be the weighted degree function with weight 0 to any generator of A_* and weight 1 to ∂. Thus this weighted degree of $f \in R_*$ coincides with the degree of f in R. Such degree is clearly invariant under the multiplication of elements in A_*.

Lemma 3.8. Let $M \in R^{g \times q}$. Then there exists an algorithm to compute a R-unimodular matrix $T \in R_*^{g \times g}$ such that $TM \in R_*^{g \times q}$.

Proof. If $M \in R_*^{g \times g}$, there is nothing to do. Suppose that M contains elements with fractions. At first, we show how to bring two fractional elements $a^{-1}b, c^{-1}d$ for $a, c \in A_*$, $b, d \in R_*$ to a common left denominator, cf. [1]. For any $h_1, h_2 \in A_*$, such that $h_1 a = h_2 c$, it is easy to see that

$$(h_1 a)^{-1}(h_1 b) = a^{-1}h_1^{-1}h_1 b = a^{-1}b \text{ and } (h_1 a)^{-1}(h_2 d) = (h_2 c)^{-1}(h_2 d) = c^{-1}d,$$

hence $(h_1 a)^{-1} = a^{-1}h_1^{-1} = (h_2 c)^{-1}$ is a common left denominator. Analogously we can compute a common left denominator for any finite set of fractions. Let T_{ii} be a common left denominator of non-zero elements from the i-th row of M, then TM contains no fractions. Moreover, T is a diagonal matrix with non-zero polynomial entries, so it is R-unimodular. $\square$

Remark 3.9. Note that the computation of compatible factors h_i for $a_1, a_2 \in A_*$ can be achieved by computing syzygies, since $\{(h_1, h_2) \in A_*^2 \mid h_1 a_1 = h_2 a_2\}$ is exactly the module $Syz(a_1, -a_2) \subset A_*^2$. The factors h_i for more a_i's can be obtained as well.

Define $M_* := TM \in R_*^{p \times q}$ using the notation of Lemma 3.8. Then the relations $_{R_*}M_* \subseteq {}_RM$ and $_RM_* = {}_RM$ hold obviously. Thus whenever we speak about a finitely generated submodule $_RM \subset R^{1 \times q}$, we denote by $_RM_*$ a presentation of $_RM$ with generators contained in R_*. In what follows, we will show how to find R-unimodular matrices $U \in R_*^{p \times p}$ and $V \in R_*^{q \times q}$ such that

$$U(TM)V = \begin{bmatrix} r_1 & & & \\ & \ddots & & \\ & & r_q & \\ & & & 0 \end{bmatrix} \in R_*^{p \times q}.$$

Since the equality $U(TM)V = (UT)MV$ holds and UT is a R-unimodular matrix, our initial aim follows.

As in the previous subsection, by $\mathcal{G}(_{R_*}M_*)$ we denote the reduced left Gröbner basis of the submodule $_{R_*}M_*$ with respect to the module ordering $<_*$ on R_*, which was already defined in (1). Unlike the rational case, the leading monomials of elements in $R_*^{1 \times g}$ are of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \partial^\beta$ for $\alpha_i, \beta \in \mathbb{N}$.

Remark 3.10. Using the polynomial strategy, two improvements can be observed. On the one hand, once we have mapped the matrix we work with from $R^{g \times q}$ to $R_*^{g \times q}$, the complicated arithmetics in the skew field of fractions is not used anymore. The other improvement lies in the nature of construction of normal forms for matrices and the corresponding transformation matrices. The naive approach would be to apply elementary operations inclusive division by invertibles on the rows and columns, that is, operations from the left and from the right. Indeed, there are methods using different techniques like, for instance, p-adic arguments to calculate the invariant factors of the Smith form over integers [26], but this method does not help in construction of transformation matrices. Surely the swap from left to right has no influence in the commutative framework. But already in the rational Weyl algebra B_1 (see Example 2.3), $\frac{1}{x}$ is an unit in B_1 and $\partial \frac{1}{x} = \frac{1}{x}\partial - \frac{1}{x^2}$. Comparing the multiplication with the inverse element, that is, with x, we see that $\partial x = x\partial + 1$ holds. Thus a multiplication of any polynomial containing ∂ with the element $\frac{1}{x}$ in the field of fractions causes an immediate coefficient swell. Since a normal form of a matrix is given modulo unimodular operations, the previous example illustrates the variations of possible representations. In section 4, we present nontrivial examples. Especially in the Example 4.10, the polynomial strategy dams up the coefficient increase in a very impressive way.

On the other hand, switching to the polynomial framework changes the setup. The ring R_* is not a PID anymore, what was the essential property for the existence of a diagonal form over R. In the sequel, we show how that this problem can be resolved by introducing a suitable sorting condition for the chosen module ordering. Referring to the argumentation of Remark 3.3 yields the block-diagonal form with the 0 block above.

$$\mathcal{G}(_{R_*}M_*) = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \boxed{*} & & & \\ \vdots & & 0 & \\ * & & & \\ & \boxed{*} & & \\ & \vdots & & 0 \\ & * & & \\ & & \ddots & \\ & & & \boxed{*} \\ & * & & \vdots \\ & & & * \end{bmatrix}. \tag{2}$$

Moreover, the rows with the boxed element have the smallest leading monomial with respect to the chosen ordering in the corresponding block. A block denotes all elements of same leading position in $\mathcal{G}(_{R_*}M_*)$. In Theorem 3.15 we show that these elements indeed generate $_RM$, while in Lemma 3.13 we show that these elements provide us with additional information. However, this result requires some preparations.

Lemma 3.11. Let P be R or R_*. For $M \in P^{g \times q}$ of full rank and every $1 \leq i \leq g$, define $\alpha_i := \min\{\deg(a) \mid a \in {}_P M \setminus \{0\}$ and $\text{lpos}(a) = i\}$. Then for all $1 \leq i \leq g$, there exists $h_i \in \mathcal{G}({}_P M)$ of degree α_i with $\text{lpos}(h_i) = i$.

Proof. Recall that $\partial \gg x_j$ for all j. Let $f \in {}_P M$ with $\text{lpos}(f) = i$ and $\deg(f) = \alpha_i$. Suppose that for all $g \in \mathcal{G}({}_P M)$ with leading position i, $\deg(g) > \alpha_i$ holds. Since $\mathcal{G}({}_P M)$ is a Gröbner basis, there exists $g \in \mathcal{G}({}_P M)$ such that $\text{lm}(g)$ divides $\text{lm}(f)$. This happens if and only if $\deg(g) \leq \deg(f)$ (because R_* is a G-algebra and R is an Ore PID), which yields a contradiction. $\square$

The full rank assumption in the lemma guarantees the existence of α_i for each component $1 \leq i \leq g$. Note, that over R_* the cardinality of $\{\deg(a) \mid a \in {}_P M \setminus \{0\}$ and $\text{lpos}(a) = i\}$ is more than one in general, hence there might be different selection strategies. We propose to select an element according to $\min_{<_*}$, see Lemma 3.13.

Corollary 3.12. Lemma 3.11 and Lemma 3.3 yield

$$\deg(\mathcal{G}({}_R M)_i) = \min\{\deg(a) \mid a \in {}_R M \setminus \{0\} \text{ and } \text{lpos}(a) = i\}.$$

Lemma 3.13. Let α_i be the degree of the boxed entry with leading position in the i-th column, that is

$$\alpha_i := \deg(\min_{<_*}\{b \mid b \in \mathcal{G}({}_{R_*} M_*) \text{ and } \text{lpos}(b) = i\}).$$

Then for all $h \in {}_R M$ with $\text{lpos}(h) = i$ we have $\deg(\text{lm}(h)) \geq \alpha_i$.

Proof. Now suppose the claim does not hold and there is $h \in {}_R M$ with $\text{lpos}(h) = i$ of degree smaller than α_i. Using Lemma 3.8, there exists $a \in A_*$ such that $ah \in {}_{R_*} M_*$. Then $\deg(ah) = \deg(h)$ and $\text{lpos}(ah) = i$. Due to Lemma 3.11, $\deg(f) \geq \alpha_i$ for all $f \in {}_{R_*} M_*$ with leading position i, hence we obtain a contradiction. $\square$

Corollary 3.14. Lemma 3.13 and Corollary 3.12 imply, that $\forall\, 1 \leq i \leq g$

$$\min\{\deg(a) \mid a \in {}_R M \setminus \{0\} \wedge \text{lpos}(a) = i\} = \min\{\deg(a) \mid a \in {}_{R_*} M_* \setminus \{0\} \wedge \text{lpos}(a) = i\}.$$

Theorem 3.15. Let $M \in R^{g \times g}$ be of full rank. For each $1 \leq i \leq g$, let us define

$$b_i := \min_{<_*}\{b \mid b \in \mathcal{G}({}_{R_*} M_*) \text{ and } \text{lpos}(b) = i\}.$$

Since M is of full rank, the minimum exists for each $1 \leq i \leq g$. Note that the set $\{b_1, \ldots, b_g\}$ corresponds to the subset of all rows with a boxed entry in the block triangular form 2. Moreover ${}_R \langle b_1, \ldots, b_g \rangle = {}_R M$.

Proof. Let $f \in {}_R M \setminus \{0\}$. Due to Corollary 3.14, there exists $1 \leq k \leq g$ such that $\text{lpos}(b_k) = \text{lpos}(f)$ and $\deg(b_k) \leq \deg(f)$. Thus there exists an element $s_k \in R$ such that $\deg(f - s_k b_k) < \deg(b_k)$. Since $f - s_k b_k \in {}_R M$, Corollary 3.14 implies that we have $\text{lpos}(f - s_k b_k) < \text{lpos}(f)$. Iterating this reduction leads to the remainder zero and thus $f = \sum_{i=1}^{k} s_i b_i$. $\square$

Using the notation of the previous theorem, let $G^*(_RM) := [b_1, \ldots, b_g]^T$, which is by definition a lower triangular matrix. In the sequel, let $M \in R^{g \times g}$ be of full rank. Note that then obviously $G^*(_RM)$ is a square matrix.

Proposition 3.16. Suppose $M \in R^{g \times g}$ is a full rank matrix and there is $U_* \in R_*^{l \times g}$ such that $U_*M_* = \mathcal{G}(_{R_*}M_*)$. Let us select the indices

$$\{t_1, \ldots, t_g\} \subseteq \{1, \ldots, l\} \text{ such that } \{(U_*M_*)_{t_1}, \ldots, (U_*M_*)_{t_g}\} = G^*(_RM) \quad (3)$$

in the notation of Theorem 3.15. Then $U := [(U_*)_{t_1}, \ldots, (U_*)_{t_g}]^T$ is R-unimodular in $R^{g \times g}$ and $UM_* = G^*(_RM)$.

Proof. The equality $UM_* = G^*(_RM)$ follows by the definition of U. Now we show that U is R-unimodular. Note that $_R(UM_*) = {}_RG^*(_RM) = {}_RM = {}_RM_*$ holds and $UM_* \subset R^{g \times g} \supset M_*$. Thus there exists $V \in R^{g \times g}$ such that $M_* = V(UM_*)$. Then $VU = \mathrm{id}_{g \times g}$ and analogously $UV = \mathrm{id}_{g \times g}$ since M has full row rank. $\square$

Lemma 3.17. The equality of the following left ideals holds:

$$_R\langle \theta(G^*(_RM)_{g1}), \ldots, \theta(G^*(_RM)_{gg}) \rangle = {}_R\langle G^*(\widetilde{\theta}(G^*(_RM))_{gg} \rangle.$$

Proof. Using the argumentation given in the proof of Lemma 3.4 we obtain

$$_R\langle \theta(G^*(_RM)_{g1}), \ldots, \theta(G^*(_RM)_{gg}) \rangle = {}_R\langle \mathcal{G}(\widetilde{\theta}(G^*(_RM))_{gg} \rangle.$$

Note the module identities $_RG^*(_RM) = {}_R\mathcal{G}(_RM) \Rightarrow$

$$\widetilde{\theta}(G^*(_RM))_R = \widetilde{\theta}(\mathcal{G}(_RM))_R \Rightarrow {}_RG^*(\widetilde{\theta}(G^*(_RM))) = {}_R\mathcal{G}(\widetilde{\theta}(\mathcal{G}(_RM))).$$

According to the latter identity and to the fact that both $\mathcal{G}(\widetilde{\theta}(\mathcal{G}(_RM))$ and $G^*(\widetilde{\theta}(G^*(_RM)))$ are lower triangular matrices, we obtain $_R\langle \mathcal{G}(\widetilde{\theta}(\mathcal{G}(_RM))_{gg} \rangle = {}_R\langle G^*(\widetilde{\theta}(G^*(_RM))_{gg} \rangle.$ $\square$

Now we are ready to formulate the polynomial version of Algorithm 3.5.

Algorithm 3.18 (Polynomial diagonalization with Gröbner Bases).
Input: $M \in R^{g \times g}$ of full rank, θ an involution on R_* and $\widetilde{\theta}$ as above.
Output: R-unimodular matrices $U, V, D \in R_*^{g \times g}$ such that $U \cdot M \cdot V = D = \mathrm{Diag}(r_1, \ldots, r_g)$.

    Find $T \in R^{g \times g}$ unimodular such that $TM \in R_*^{g \times g}$
    $M^{(0)} \leftarrow TM, \quad U \leftarrow T, \quad V \leftarrow \mathrm{id}_{g \times g}$
    $i \leftarrow 0$
    while $M^{(i)}$ is not a diagonal matrix **or** $i \equiv_2 1$ **do**
      $i \leftarrow i + 1$
      Compute $U^{(i)}$ so that $U^{(i)} \cdot M^{(i-1)} = \mathcal{G}(_{R_*} M^{(i-1)}) \in R_*^{l \times g}$
      Select $\{t_1, \ldots, t_g\} \subseteq \{1, \ldots, l\}$ as in (3)
      $U^{(i)} \leftarrow [(U^{(i)})_{t_1}, \ldots, (U^{(i)})_{t_g}]^T$
      $M^{(i)} \leftarrow \widetilde{\theta}(G^*(_R M))$
      if $i \equiv_2 0$ **then**
        $V \leftarrow V \cdot \widetilde{\theta}(U^{(i)})$
      else
        $U \leftarrow U^{(i)} \cdot U$
      end if
    end while
    return $(U, V, M^{(i)})$

Remark 3.19. It is important to mention, that the matrices U, V, D (hence the elements r_i as well) have entries from R_*, that is polynomials. However, U and V are only unimodular over R and, in general, they need not be unimodular over R_* for obvious reasons. In each presented example we will investigate the case, whether U or V will be unimodular over R_* as well. After all, we come up with the Conjecture 4.13.

Theorem 3.20. Algorithm 3.18 terminates with the correct result.

Proof. Using Proposition 3.16 and replacing Lemma 3.4 by Lemma 3.17 in the proof of Theorem 3.6 provides the claim. $\square$

Example 3.21. Suppose $R = K(x)[\partial; \mathrm{id}, \frac{d}{dx}]$ and $R_* = K[x][\partial; \mathrm{id}, \frac{d}{dx}]$. Let us define an involution on R_* by $\theta(\partial) = -\partial$ and $\theta(x) = x$. Let

$$M = \begin{bmatrix} \partial^2 - 1 & \partial + 1 \\ \partial^2 + 1 & \partial - x \end{bmatrix} \in R^{2 \times 2}.$$

Evidently $T = \mathrm{id}_{2 \times 2}$ and thus $M^{(0)} := M$, $U = V = \mathrm{id}_{2 \times 2}$ and $i = 0$.

   1: Since $M^{(0)}$ is not diagonal, go into the while loop

      • $i \leftarrow 1$. Since $\begin{bmatrix} -x\partial - \partial + x^2 + x + 1 & x\partial + \partial + x \\ -\partial^2 + x\partial - \partial + x + 2 & \partial^2 + 2\partial + 1 \\ \partial - x & -\partial - 1 \end{bmatrix} M^{(0)} = \mathcal{G}(_{R_*} M^{(0)})$

        where $\mathcal{G}(_{R_*} M^{(0)}) = \begin{bmatrix} x^2\partial^2 + 2x\partial^2 + \partial^2 + 2x\partial + 2\partial - x^2 - 1 & 0 \\ x\partial^3 + \partial^3 + x\partial^2 + 5\partial^2 - x\partial + 3\partial - x - 1 & 0 \\ -x\partial^2 - \partial^2 - 2\partial + x - 1 & 1 \end{bmatrix}$ and

        $i \equiv_2 1$

17

$$M^{(1)} \leftarrow \left[\begin{array}{cc} x^2\partial^2 + 2x\partial^2 + \partial^2 + 2x\partial + 2\partial - x^2 - 1 & -x\partial^2 - \partial^2 + x - 1 \\ 0 & 1 \end{array} \right]$$

$$U \leftarrow \left[\begin{array}{cc} -x\partial - \partial + x^2 + x + 1 & x\partial + \partial + x \\ \partial - x & -\partial - 1 \end{array} \right]$$

2: Since $M^{(1)}$ is not diagonal, go into the while loop

- $i \leftarrow 2$. Since $\left[\begin{array}{cc} 1 & x\partial^2 + \partial^2 - x + 1 \\ 0 & 1 \end{array} \right] M^{(1)} = \mathcal{G}(_{R_*} M^{(1)})$ and $i \equiv_2 0$

$$M^{(2)} \leftarrow \left[\begin{array}{cc} x^2\partial^2 + 2x\partial^2 + \partial^2 + 2x\partial + 2\partial - x^2 - 1 & 0 \\ 0 & 1 \end{array} \right],$$

$$V \leftarrow \left[\begin{array}{cc} 1 & 0 \\ (x+1)\partial^2 + 2\partial - x + 1 & 1 \end{array} \right]$$

3: Since i is even and $M^{(2)}$ is diagonal, the algorithm returns U and V.

And indeed, the algorithm outputs the claimed result, since

$$UMV = \left[\begin{array}{cc} x^2\partial^2 + 2x\partial^2 + \partial^2 + 2x\partial + 2\partial - x^2 - 1 & 0 \\ 0 & 1 \end{array} \right].$$

In view of Remark 3.19, let us analyze the transformation matrices for R_*-unimodularity. Indeed, V is such since it admits an inverse V'. On the contrary, U is only unimodular over R and not over R_*, since $U \cdot Z = W$ and W is first invertible in the localization:

$$V' = \left[\begin{array}{cc} 1 & 0 \\ -(x+1)\partial^2 + x - 2\partial - 1 & 1 \end{array} \right], Z = \left[\begin{array}{cc} 2\partial + 2 & (x+1)\partial + x - 2 \\ 2(\partial - x) & (x+1)\partial - x^2 - x - 3 \end{array} \right],$$

$$W = \left[\begin{array}{cc} 0 & -4x^2 - 8x - 4 \\ 2 & 5x + 5 \end{array} \right].$$

Algorithm 3.18 can be extended to $M \in R^{g \times q}$ along the lines already presented in Remark 3.7.

Example 3.22. By executing the algorithm in the 1st rational shift algebra $K\langle t, S \mid St = tS + S \rangle$ on the same matrix as in the previous example, where ∂ is replaced with the forward shift operator S, we obtain a diagonal form
Diag$((t^2 + 3t + 2)S^2 + 2(t+1)S - t^2 - t + 2, 1) =$

$$\left[\begin{array}{cc} -tS - S + t^2 + 2t & tS + S + t + 2 \\ -S + t + 1 & S + 1 \end{array} \right] \cdot \left[\begin{array}{cc} S^2 - 1 & S + 1 \\ S^2 + 1 & S - t \end{array} \right] \cdot \left[\begin{array}{cc} 1 & 0 \\ -tS^2 - 2S^2 - 2S + t & 1 \end{array} \right].$$

As in the previous example, it turns out that V (but not U) is even R_*-unimodular.

4 Implementation and Examples

4.1 Jacobson Form

Let R be a left and right Euclidean domain. Inspired by the Smith form, we will focus on how to sharpen the result of the already discussed diagonal form.

Theorem 4.1. [10, 20] Every matrix $M \in R^{g \times q}$ is associated to a certain diagonal matrix, namely $\text{Diag}(m_1, \ldots, m_\ell, 0, \ldots, 0)$ such that additionally

$$Rm_{i+1}R \subseteq m_i R \cap Rm_i \qquad (4)$$

holds for all $i = 1, \ldots, \min\{g, q\} - 1$.

Due to [20, Theorem 31] the elements m_i are unique up to similarity. Two elements m_i and n_i are called **similar** if and only if there exist $a, b \in R$ such that

$$am_i = n_i b, \quad R = aR + n_i R, \quad R = Rb + Rm_i.$$

Using the notation of the previous theorem, we call $\text{Diag}(m_1, \ldots, m_\ell, 0, \ldots, 0)$ a **Jacobson normal form** of M. Note that (4) is hard to tackle constructively in general, since it requires to work with the intersection of a left and a right ideal. This difficulty disappears if R has only trivial two-sided ideals, that is when R is simple. Then each matrix M possesses a Jacobson form $\text{Diag}(1, \ldots, 1, m_M, 0, \ldots, 0)$ with $m_M \in R$.

Lemma 4.2. Let A_* be a G-algebra, $A = \text{Quot}(A_*)$ and $R = A[\partial; \sigma, \delta]$. Let U, V be unimodular and $a, b, c, d \in R \setminus \{0\}$ such that

$$U \, \text{Diag}(a, b) V = \text{Diag}(c, d). \qquad (5)$$

Then $\deg(a) + \deg(b) = \deg(c) + \deg(d)$.

Proof. Due to (5) there exists a R-module isomorphism

$$\phi : R/aR \oplus R/bR \to R/cR \oplus R/dR.$$

Since A is a skew field, ϕ induces an A-vector space isomorphism. Thus the A-dimensions of $R/aR \oplus R/bR$ and $R/cR \oplus R/dR$, which are nothing else that the sums of degrees, coincide. $\qquad \square$

Of course, inductive argument implies that sums of degrees of diagonal entries of two diagonal presentation matrices of the same module are the same.

Jacobson normal form in the 1st Weyl algebra. Let R be the rational Weyl algebra $K(x)[\partial; 1, \frac{\partial}{\partial x}]$, which is a simple domain.

Lemma 4.3. Consider $a, b \in R$ with $\deg(a) > 0$, $b \neq 0$ and $\deg(b) \geq \deg(a)$. Then there exists $i \in \{0, \ldots, \deg(b) - \deg(a) + 1\}$ such that a is not a strict right divisor of bx^i.

Proof. Suppose that for every $i \in \{0, \ldots, \deg(b) - \deg(a) + 1\}$ there exists a $q_i \in R$ such that $bx^i = q_i a$. Let $b = b_n(x)\partial^n + \cdots + b_1(x)\partial + b_0(x)$. Note, that for any $k \in \mathbb{N}$ the equality $\partial^k x = x\partial^k + k\partial^{k-1}$. Thus we define $r_1 := bx - xb = \sum_{i=1}^n b_i(x)i\partial^{i-1}$ with $\deg(r_1) = n - 1 < \deg(b)$ and $r_1 \neq 0$ since $\deg(b) \geq 1$. Since $b = q_0 a$ and $bx = q_1 a$, it follows that $r_1 = bx - xb = (q_1 - q_0 x)a$, that is

19

a is a strict right divisor of r_1. By proceeding with bx^2 and so on, we obtain a sequence of non-zero polynomials r_i, such that $\deg(b) > \deg(r_1) > \ldots$ and a is a strict right divisor of r_i. Since the degree of r_i decreases exactly by 1 at each step, after at most $\deg(b) - \deg(a) + 1$ iterations we obtain a polynomial of degree $\deg(a) - 1$, which is non-zero. Such a polynomial must contain a right factor of degree $\deg(a)$, what is a contradiction. $\qquad\square$

The Lemma (4.3) suggests an algorithm to compute the Jacobson form from a diagonal matrix over the rational Weyl algebra. Suppose $M \in R^{g \times q}$, where $g = q = 2$. The extension to $g, q \in \mathbb{N}$ is evident. Algorithm 3.18 returns unimodular matrices U, V such that $UMV = \text{Diag}(m_1, m_2)$. Without loss of generality, assume that $\deg(m_2) \leq \deg(m_1)$.

1) If m_2 is a unit, we get the Jacobson form just by replacing U by $\text{Diag}(1, m_2^{-1})U$. Otherwise, choose an exponent $i \in \mathbb{N}$ (it exists by the Lemma 4.3) such that $m_1 x^i = am_2 + b$ with $\deg(b) < \deg(m_2)$ and $b \neq 0$. Then

$$\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m_1 & 0 \\ 0 & m_2 \end{bmatrix} \cdot \begin{bmatrix} 1 & x^i \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 & b \\ 0 & m_2 \end{bmatrix}.$$

Replace U by $\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} U$ and V by $V \begin{bmatrix} 1 & x^i \\ 0 & 1 \end{bmatrix}$.

2) Now we apply Algorithm 3.18 to the matrix $\begin{bmatrix} m_1 & r \\ 0 & m_2 \end{bmatrix}$. The result is then
$\text{Diag}(m_1', m_2')$, where $\deg(m_2') < \deg(m_2)$.

Thus, by iterating 1) and 2) we compute U and V, such that $UMV = \text{Diag}(1, m_M)$.

Remark 4.4. It seems to us, that the process of obtaining Jacobson normal form from an appropriate diagonal matrix can be generalized to any constructive simple Euclidean PID. Moreover, it can be applied even over non-simple domains. There, it is not guaranteed, that the result is so nice as Jacobson form, but the procedure above can simplify diagonal matrices.

Example 4.5. Over the first rational shift algebra $A = K(t)\langle s \mid st = ts + s \rangle$ (which is a not a simple domain), we provide a counterexample for a statement, similar to 4.3. Consider the 2×2 diagonal matrix $D_1 = \text{Diag}(s, s)$. Then the left module $M_1 = A^2/A^2 D_1$ (it is of dimension 2 over $K(t)$) is annihilated by the two-sided ideal $\langle s \rangle$ and hence D_1 is not equivalent to a matrix of the form $D_2 = \text{Diag}(1, p)$. If it were so, due to the $K(t)$-dimension of M_1 and hence $M_2 = A^2/A^2 D_2$, we see that $\text{lm}(p) = s^2$. Since $M_2 = A^2/A^2 \text{Diag}(1, p) \cong A/Ap$, we have $\text{Ann}_A M_2 = \langle p \rangle$.

Since it is not equal to $\text{Ann}_A M_1 = \langle s \rangle$, $M_1 \not\cong M_2$. Hence, unlike over the Weyl algebra (or a simple domain [10]), there are many different types of normal forms even for diagonal matrices.

Example 4.6. Consider the rational q-Weyl algebra, cf. 2.3. It is not simple since e. g. the ideal $\langle (q-1)\partial + x^{-1} \rangle$ is a proper two-sided ideal. Denote the generator by f, then, by the same argumentation as in the previous example we can show, that $\mathrm{Diag}(f, f)$ is not equivalent to any matrix of the type $\mathrm{Diag}(1, g)$.

Since little is known about normal forms of non-simple domains, this approach is very interesting to investigate in the future.

Cyclic vector method. Indeed, the existence of Jacobson form in simple Euclidean PID is very strong result. In particular, it tells us that any finitely generated module is cyclic and its presentation is a principal ideal. The method of finding a cyclic vector in a module and obtain a left ideal, annihilating it, is used in D-module theory. J. Middeke in [28] did some investigations of this question.

Conjecture 4.7. We conjecture, that the Jacobson form for, say, square matrix M over a simple Euclidean domain R can be computed from the given diagonal form in the following way. Let $M = \mathrm{Diag}(m_1, \ldots, m_r)$. Since $\sum \deg(m_i)$ is invariant of the module $R^{r \times r}/M$, this number can be used as a certificate for probabilistic approach. Namely, consider polynomials p_i of degree at most $\deg(m_i) - 1$ with random coefficients in A. Compute a generator $c \in R$ of the left annihilator ideal of a vector $[p_1, \ldots, p_r]^T$ in $R^{r \times r}/M$. If $\deg c = \sum \deg(m_i)$, then $\mathrm{Diag}(1, \ldots, 1, c)$ is a Jacobson form of M. Otherwise one takes another set of random polynomials p_i and repeats the procedure.

One needs the probabilistic estimations on the length of random coefficients like in [21].

4.2 Examples, Applications and Comparison

Implementations of Jacobson normal form. To the best of our knowledge, Jacobson normal form algorithm has been implemented in MAPLE by Culianez and Quadrat [11], by Robertz et al. [4, 8], by Middeke [28] and by Cheng et al [3, 6, 12].

We could not locate the download version of the implementation of [11]. The packages FFREDUCE [3] and MODREDUCE [6] are available via personal request to their authors. The implementation of J. Middeke [28] was, according to its author, merely a check of ideas and was not supposed to become a freely distributed package for MAPLE. This package is able to compute in the 1st Weyl algebra with coefficients in a differential field.

D. Robertz informed us, that his implementation [4] directly follows the classical algorithm and it has not been specially optimized. Nevertheless, in what follows, we compare our implementation with the one in the MAPLE package JANET [4] on some nontrivial examples. This package is available to general

public.

In packages by H. Cheng et al. modular (MODREDUCE) and fraction-free (FFREDUCE) versions of an order basis of a polynomial matrix M from an Ore algebra A are implemented. In particular, such a basis is used to compute the left nullspace of M, and indirectly the Popov form of M.

Examples. As we already pointed out in the introduction, behind diagonalized matrices and normal forms there are various application-driven motivations, see e. g. [11].

Example 4.8. For instance, consider a double pendulum with lengths ℓ_1 and ℓ_2. Thus ℓ_1, ℓ_2 and g are constants, that is non-zero elements of K (for details see [11], Example 3.2.2). The linearization of this problem leads to the system of linear partial differential equations in $\partial = \frac{\partial}{\partial t}$, which can be written in the matrix form with the matrix

$$M = \begin{bmatrix} \ell_1\partial^2 + g & 0 & -g \\ 0 & \ell_2\partial^2 + g & -g \end{bmatrix}.$$

Since the variable t does not appear in M, the ground ring for the diagonalization process can be thought as of $A = \mathbb{Q}(\ell_1, \ell_2, g)[\partial]$. Thus, indeed one can compute the Smith normal form.

Our implementation of the diagonal form of M on this example returns

$$U = \begin{bmatrix} -1/g & 0 \\ -1/g & 1/g \end{bmatrix} \text{ and } V = \begin{bmatrix} 0 & g\ell_2 & -g\ell_2\partial^2 - g^2 \\ 0 & g\ell_1 & -g\ell_1\partial^2 - g^2 \\ 1 & \ell_1\ell_2\partial^2 + g\ell_2 & -\ell_1\ell_2\partial^4 - g\ell_1 - g\ell_2\partial^2 - g^2 \end{bmatrix}$$

such that

$$UMV = \begin{bmatrix} 1 & 0 & 0 \\ 0 & g\ell_1 - g\ell_2 & 0 \end{bmatrix}.$$

This result agrees with results, obtained in [11]. Note, that a purely fractional method (as well as coefficient normalization procedure) will return 1 instead of $g(\ell_1 - \ell_2)$. With our polynomial approach we obtain a polynomial matrix, which is useful for further investigations. In particular, in the current example we see, that setting $\ell_1 = \ell_2$ implies the drop of the rank of the Smith form from 2 to one, thus the properties of the corresponding system will change. In control theory one establishes quite different properties of the module in the non-generic case $\ell_1 = \ell_2$.

Remark 4.9. In [25] the algorithm for finding so-called "obstructions to genericity" was derived and discussed. A lesson learned from that paper can be applied for an implementation of Jacobson form as follows. It is recommended to split the algorithm (resp. the implementation) into two parts. In the first part one computes a diagonal matrix, where the invertibles of the ground ring are not canceled artificially. The second part applies the normalization on the invertibles; this part is trivial to achieve. Note, that our polynomial algorithm allows one to keep a close track on suspicious invertibles due to this scheme.

Example 4.10. Over the first rational Weyl algebra $\mathbb{Q}(t)[\partial; \mathrm{id}, \frac{d}{dt}]$, consider the matrix

$$R = \begin{bmatrix} \partial^2 & \partial + 1 & 0 \\ \partial + 1 & 0 & \partial^3 - t^2\partial \\ 2\partial + 1 & \partial^3 + \partial^2 & \partial^2 \end{bmatrix}.$$

A typical implementation of the Jacobson normal form returns the matrix $D = \mathrm{Diag}(g, 1, 1)$ together with transformation matrices $U, V \in \mathbb{Q}[t][\partial; \mathrm{id}, \frac{d}{dt}]^{3\times 3}$ such that $URV = D$. Below, we write down just the leading term of each matrix entry and moreover, we write "l.o.t." for "lower order terms" with respect to degree lexicographical ordering on $\mathbb{Q}[t][\partial; \mathrm{id}, \frac{d}{dt}]$. The implementation of the Algorithm 3.18 in SINGULAR returns $D = \mathrm{Diag}(2t^2 d^8 + 33 \text{ l.o.t.}, 1, 1)$. The transformation matrices are

$$U = \begin{bmatrix} \frac{1}{2}t\partial^{13} + 24 \text{ l.o.t.} & \frac{1}{2}t\partial^{10} + 19 \text{ l.o.t.} & \frac{1}{2}t\partial^{11} + 44 \text{ l.o.t.} \\ \frac{1}{2} & 0 & 0 \\ -\frac{1}{4}\partial^5 + 2 \text{ l.o.t.} & -\frac{1}{4}\partial^2 & \frac{1}{4} + 2 \text{ l.o.t.} \end{bmatrix},$$

and

$$V = \begin{bmatrix} 2t\partial^2 + 3 \text{ l.o.t.} & 2\partial^2 & 2\partial^2 + 1 \text{ l.o.t.} \\ -2t\partial^3 + 2 \text{ l.o.t.} & -2\partial^3 + 3 \text{ l.o.t.} & -2\partial^3 \\ t\partial^8 + 28 \text{ l.o.t.} & \partial^8 + 11 \text{ l.o.t.} & \partial^8 + 16 \text{ l.o.t.} \end{bmatrix}.$$

In view of 3.19, V (but not U) is unimodular over $R_* = \mathbb{Q}[t][\partial; \mathrm{id}, \frac{d}{dt}]$.

JANET returns a matrix $\mathrm{Diag}(1, 1, (279936t^{14} + 14 \text{ l.o.t.})^{-1}(279936t^{14}\partial^8 + 145 \text{ l.o.t.}))$,

$$U = \begin{bmatrix} 1 & 0 & 0 \\ (6t^2 + 2 \text{ l.o.t.})^{-1}(\partial^2 + 1 \text{ l.o.t.}) & (6t^2 + 2 \text{ l.o.t.})^{-1}(\partial^3 + 3 \text{ l.o.t.}) & (6t^2 + 2 \text{ l.o.t.})^{-1} \\ u_{31} & u_{32} & u_{33} \end{bmatrix},$$

where $g = (559872t^{14} + 14 \text{ l.o.t.})$, $u_{31} = g^{-1}(-279936t^{14}\partial^9 + 158 \text{ l.o.t.})$, $u_{32} = g^{-1}(279936t^{14}\partial^{10} + 182 \text{ l.o.t.})$, $u_{33} = g^{-1}(279936t^{14}\partial^7 + 127 \text{ l.o.t.})$. The right transformation matrix $V =$

$$\begin{bmatrix} 1 & \frac{1}{2}\partial^6 + 15 \text{ l.o.t.} & (279936t^{14} + 14 \text{ l.o.t. })^{-1}(46656t^{12}\partial^7 + 110 \text{ l.o.t. }) \\ \partial + 1 \text{l.o.t.} & -\frac{1}{2}\partial^7 + 15 \text{ l.o.t.} & (-1679614t^{16} + 16 \text{ l.o.t. })^{-1}(279936t^{14}\partial^8 + 138 \text{ l.o.t. }) \\ 0 & 1 & (6t^2 + 2 \text{ l.o.t. })^{-1}(2\partial^2 + 1 \text{ l.o.t }) \end{bmatrix}.$$

Example 4.11. Consider the matrix from the Example 4.10, replacing ∂ by S, the forward shift operator in the first rational shift algebra in t, s. Then the diagonal form, computed with our algorithm is $\mathrm{Diag}(t^{12}S^8 + 101 \text{ l.o.t.}, 1, 1)$. Notably, the leading coefficient in t factorizes completely. Transformation matrices are, as expected, more complicated as in the Example 4.10. U has only three entries of length bigger than 1; their lengths are 113, 116, 150. In the matrix V, the lengths of entries are 22, 11, 58, 20, 14, 60, 26, 17, 64 with degree in S up to 7. Coefficients, having more than 7 digits appear only in one entry, and grow up to 12 digits. The situation in the first rational difference algebra is similar, as a reader can see by computing with our implementation. We have computed all the examples from this paper in the shift and difference settings as well.

Example 4.12. Let $R = \mathbb{Q}(y,x)[\partial; \mathrm{id}, \frac{d}{dx}]$ and thus $R_* = \mathbb{Q}[y,x][\partial; \mathrm{id}, \frac{d}{dx}]$. The matrix M below comes from the system of partial differential equations. With our algorithm we obtain transformation matrices and a diagonal one:

$$M = \begin{bmatrix} y^2\partial^2 + \partial + 1 & 1 \\ x\partial & x^2\partial^2 + \partial + y \end{bmatrix},$$

$$\begin{bmatrix} -x^2\partial^2 - \partial - y & 1 \\ 1 & 0 \end{bmatrix} M \begin{bmatrix} 1 & 0 \\ -y^2\partial^2 - \partial - 1 & 1 \end{bmatrix} = \begin{bmatrix} g & 0 \\ 0 & 1 \end{bmatrix},$$

where $g = -y^2x^2\partial^4 - x^2\partial^3 - x^2\partial^2 - y^2\partial^3 + x\partial + (-y^3 - 1)\partial^2 + (-y - 1)\partial - y$.

If we consider $M \in \mathbb{Z}_2(y,x)[\partial; \mathrm{id}, \frac{d}{dx}]^{2\times 2}$, we obtain the single example from [28]. Then the rational form of our result is exactly the result obtained in [28], namely $\mathrm{Diag}(1, -\frac{g}{x^2y^2} \mod 2)$. Note, that in our method no computations with 4×4 matrices as in [28] are needed. As demonstrated, our implementation works over finite fields as well. And, as before, the right transformation matrix V is unimodular even over $R_* = \mathbb{Q}[y,x][\partial; \mathrm{id}, \frac{d}{dx}]$.

As we have seen, in all the examples above the right transformation matrix V was indeed unimodular over R_*. We observe this phenomenon for even more examples over Weyl and shift algebras.

Conjecture 4.13. Let A_* be a G-algebra and $A = \mathrm{Quot}(A_*)$. Moreover, let $R = A[\partial; \sigma, \delta]$, such that $R_* = A_*[\partial; \sigma, \delta]$ is a G-algebra. For a matrix $M \in R^{p\times p}$ there exist square matrices U, V, D with entries from R_*, such that $UMV = D$, where D is diagonal and U, V unimodular over R. If D has only one polynomial non-constant entry, then V can be chosen to be unimodular over R_*.

Application. Over R, the decomposition as above can be applied as follows. We start with a system of equations $M\omega = 0$ in unknown functions $\omega = (\omega_1, \ldots, \omega_p)$. Since U and V are unimodular over R and $UMV = \mathrm{Diag}(d_{11}, \ldots, d_{pp})$, we obtain a decoupled system $\{d_{ii}z_i = 0\}$, where $z = V^{-1}\omega$, which is equivalent to $M\omega = 0$ over R. Note, that $d_{ii} = 0$ is possible, then one calls z_i a free variable of the system in the literature (e. g. in [31]).

Let us analyze what can be done over R_*. Suppose, that V is unimodular over R_*. Then $UM\omega = 0 \Leftrightarrow DV^{-1}\omega = 0$. However, since U is not unimodular over R_*, we have implication $M\omega = 0 \Rightarrow UM\omega = 0$ only. Let T be a matrix, such that $TU = \mathrm{id}_R$, then, by a reasoning, similar to Lemma 3.8 there exists a diagonal matrix $Q = \mathrm{Diag}(\ldots, q_{ii}, \ldots)$ such that Q resp. QT have with entries from A_* resp. R_*. For simplicity, assume that A_* is commutative. Denote by S the multiplicatively closed set, generated by q, the least common multiple of $\{q_{ii}\}$. If S happens to be an Ore set in R_*, then the localization $S^{-1}R_*$ exists and U will be unimodular over $S^{-1}R_*$. Further computations happen in different branches: first in the generic $S^{-1}R_*$, where by $UM\omega = 0 \Rightarrow M\omega = 0$ and then in the case, determined by the relation $q = 0$. In the latter, one can apply the algorithm `Genericity` from [25], which delivers a disjoint decomposition of the set of zeros of q into locally closed sets L_i. One can proceed with analysis of systems $UMw = 0$ along L_i and obtain special solutions on each L_i. This

shows, that the left transformation matrix U in this setting carries essential information about the so-called singularities of a system. Note, that working over R we compute only generic information, while following the polynomial strategy over R_* allows us to make a complete description of the system.

Clearly the decoupling, provided by a diagonal form, is of big importance for solving systems of operator equations with rational coefficients and for the structural analysis, performed in the algebraic system and control theory (see e. g. Theorem 8 of [31]).

5   Conclusion and Future Work

Indeed, this paper is a part of a general program on providing effective computations within Ore localized G-algebras. Notably, polynomial strategy, which we described in details for the case of one polynomial variable, is one of the key elements of the program. There is ongoing work on the implementation of Gröbner bases for Ore localized G-algebras under the codename SINGULAR::LOCAPAL.

Polynomial strategy brings us several advantages in practical computations. One of them is the generality of the overall approach. Namely, as soon as there is an implementation of Gröbner bases for modules (and hence syzygies) over a G-algebra A, under some mild assumptions we are able to work effectively with Ore localization A_{B^*} of A with respect to a multiplicatively closed Ore set B^*, where B is a suitable G-subalgebra of A (cf. Theorem 2.6).

The question, whether direct computations with fractions of A_{B^*} will be always outperformed by the polynomial strategy, is still open. Consider, for instance, the situation, where the input matrix M is given already with rational non-commutative coefficients. Then bringing M to the fraction-free form is already a nontrivial operation (as soon as we work with non-commutative algebra), as indicated e. g. in the proof of Lemma 3.8.

In our opinion the answer to the above question depends both on the algebra A_{B^*} and on the presentation matrix M. However, in general nontrivial computation directly using fractions in the algorithm might cause the appearance of enormous coefficients, as several examples demonstrate. We want to stress, that these examples have not been specially selected for this purpose; instead, we picked a couple of them from a bigger family of examples. In our opinion, this phenomenon is quite ubiquitous.

Our implementation of the Jacobson normal form will be developed further to provide a user with the possibility to compute in more general algebras. At the moment, the stable version of the library [30] supports first Weyl, shift and difference algebras. Investigation of normal forms over non-simple domains (as in 4.5, 4.6) is an important future task.

Middeke [28] has reported, that the classical algorithm, computing Jacobson form of a matrix over the Weyl algebra over a differential field is polynomial-time. However, it seems to us (due to polynomial strategy approach), that the

subalgebra of invertible elements must be involved in the complexity analysis. Perhaps one should consider different models for studying complexity, since experience with practical applications suggests, that the important role, played by the coefficient arithmetics (which is not the arithmetics over a numerical field anymore!) must be appropriately reflected in the overall complexity. Otherwise the complexity of operations over the skew field of invertible elements remains hidden.

Recently, Mark Giesbrecht and George Labahn suggested the use of another technique from [21], namely the randomization. Starting with a matrix M, one multiplies M with random square (hence unimodular) matrices from both sides, in order to reduce the number of iterations in the Algorithms 1 and 2. Some experiments confirm that this might be generalized to the setting of localized G-algebras. However, the computations become much harder in practice due to increased size of polynomials to deal with. This is another reason for our proposal to investigate the different notions of complexity of operations over skew fields.

Acknowledgments

References

[1] J. Apel. Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung. *Dissertation, Universität Leipzig*, 1988.

[2] M. Becker, V. Levandovskyy, and O. Yena. A SINGULAR 3.0 library for computations and operations with involutions `involut.lib`, 2003. http://www.singular.uni-kl.de.

[3] B. Beckermann, H. Cheng, and G. Labahn. Fraction-free row reduction of matrices of skew polynomials. In T. Mora, editor, *Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'02)*, pages 8–15. ACM Press, 2002.

[4] Y. A. Blinkov, C. F. Cid, V. P. Gerdt, W. Plesken, and D. Robertz. The MAPLE package "janet": II. Linear Partial Differential Equations. In *Proceedings of the 6th International Workshop on Computer Algebra in Scientific Computing*, pages 41–54, 2003. http://wwwb.math.rwth-aachen.de/Janet.

[5] J. Bueso, J. Gómez-Torrecillas, and A. Verschoren. *Algorithmic methods in non-commutative algebra. Applications to quantum groups.* Kluwer Academic Publishers, 2003.

[6] H. Cheng and G. Labahn. Modular computation for matrices of Ore polynomials. In *Computer Algebra 2006: Latest Advances in Symbolic Algorithms*, pages 43–66, 2007.

[7] F. Chyzak. Gröbner bases, symbolic summation and symbolic integration. In B. Buchberger and F. Winkler, editors, *33 years of Gröbner bases*, pages 32–60. Cambridge University Press, LMS LNS 251, 1998.

[8] F. Chyzak, A. Quadrat, and D. Robertz. OREMODULES: A symbolic package for the study of multidimensional linear systems. In J. Chiasson and J.-J. Loiseau, editors, *Applications of Time-Delay Systems*, pages 233–264. Springer LNCIS 352, 2007. http://wwwb.math.rwth-aachen.de/OreModules.

[9] F. Chyzak and B. Salvy. Non–commutative elimination in Ore algebras proves multivariate identities. *J. Symbolic Computation*, 26(2):187–227, 1998.

[10] C. Cohn. *Free Rings and their Relations.* Academic Press, 1971.

[11] G. Culianez and A. Quadrat. Formes de Hermite et de Jacobson: implementations et applications. Technical report, INRIA Sophia Antipolis, 2005.

[12] P. Davies, H. Cheng, and G. Labahn. Computing Popov form of general Ore polynomial matrices. In *Proceedings of the Milestones in Computer Algebra (MICA) Conference*, pages 149–156, 2008.

[13] J. I. García García, J. García Miranda, and F. J. Lobillo. Elimination orderings and localization in PBW algebras. *Linear Algebra Appl.*, 430(8-9):2133–2148, 2009.

[14] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Computation*, 6(2-3):149–167, 1988.

[15] G.-M. Greuel, V. Levandovskyy, and H. Schönemann. PLURAL. A SINGULAR 3.0 Subsystem for Computations with Non–commutative Polynomial Algebras. Centre for Computer Algebra, University of Kaiserslautern, 2006. http://www.singular.uni-kl.de.

[16] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.1. a Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern, 2009. http://www.singular.uni-kl.de.

[17] A. Ilchmann and V. Mehrmann. A behavioral approach to time-varying linear systems. I: General theory. *SIAM J. Control Optim.*, 44(5):1725–1747, 2006.

[18] A. Ilchmann, I. Nürnberger, and W. Schmale. Time-varying polynomial matrix systems. *Int. J. Control*, 40:329–362, 1984.

[19] M. A. Insua. *Varias perspectives sobre las bases de Gröbner: Forma normal de Smith, Algoritme de Berlekamp y álgebras de Leibniz*. PhD thesis, Universidade de Santiago de Compostela, Spain, 2005.

[20] N. Jacobson. *The Theory of Rings*. American Mathematical Society, 1943.

[21] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Mr. Smith goes to Las Vegas: Randomized parallel computation of the Smith normal form of polynomial matrices. In J. H. Davenport, editor, *Proc. EUROCAL '87*, volume 378 of *LNCS*, pages 317–322. Springer, 1989.

[22] H. Kredel. *Solvable polynomial rings*. Shaker, 1993.

[23] V. Levandovskyy. *Non-commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation.* PhD thesis, Universität Kaiserslautern, 2005. http://kluedo.ub.uni-kl.de/volltexte/2005/1883/.

[24] V. Levandovskyy and H. Schönemann. Plural — a computer algebra system for noncommutative polynomial algebras. In *Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'03)*, pages 176 – 183. ACM Press, 2003. http://doi.acm.org/10.1145/860854.860895.

[25] V. Levandovskyy and E. Zerz. Obstructions to genericity in study of parametric problems in control theory. In H. Park and G. Regensburger, editors, *Gröbner Bases in Control Theory and Signal Processing*, volume 3 of *Radon Series Comp. Appl. Math*, pages 191–214. Walter de Gruyter & Co., 2007. http://arxiv.org/abs/0708.2078.

[26] F. Lübeck. On the computation of elementary divisors of integer matrices. *J. Symbolic Computation*, 33(1):57–65, 2002.

[27] J. McConnell and J. Robson. *Noncommutative Noetherian rings*. AMS, 2001.

[28] J. Middeke. A polynomial-time algorithm for the Jacobson form for matrices of differential operators. Technical Report 2008-13, RISC, J. Kepler University Linz, 2008.

[29] M. Newman. *Integral matrices*. Academic Press, 1972.

[30] K. Schindelar and V. Levandovskyy. A SINGULAR 3.1 library with algorithms for Smith and Jacobson normal forms `jacobson.lib`, 2009. http://www.singular.uni-kl.de.

[31] E. Zerz. An algebraic analysis approach to linear time-varying systems. *IMA J. Math. Control Inf.*, 23(1):113–126, 2006.

[32] E. Zerz. State representations of time-varying linear systems. In H. Park and G. Regensburger, editors, *Gröbner Bases in Control Theory and Signal Processing*, volume 3 of *Radon Series Comp. Appl. Math*, pages 235–251. Walter de Gruyter & Co., 2007.